

CLAIMS

What is claimed is:

- 5 1. A method of producing failure alerts in a computer network containing a plurality of networked elements including at least one network router, at least one network management server, and at least one problem management server, said router being interconnected to several subnetworks, each subnetwork interconnecting several networked elements, said method comprising the steps of:
- 10 monitoring transmissions via a computer network at least one status query message to each of said networked elements in said computer network; initiating a timer for awaiting receipt of valid status responses from each networked element in reply to each status query message;
- 15 performing a fault tree analysis to determine the most likely single point of failure based upon a rule structure related to the topology of the computer network, said performance of fault tree analysis being invoked by expiration of the timer if less than all status responses are received; and
- 20 transmitting via a computer network to said problem management at least one element failed message server for said determined single point of failure such that said problem management server is notified of the most likely point of failure.

2. A method of producing failure alerts in a computer network as set forth in Claim 1 further comprising the steps of :
accessing a computer-readable media disposed in said network management server to obtain computer network connectivity and topology data; and
5 initiating said rule structure based upon said accessed computer network connectivity and topological data.
3. A method of producing failure alerts in a computer network as set forth in Claim 2, wherein the step of performing fault tree analysis further comprises the step of determining that a single element on a subnetwork is failed only if
10 no response has been received from that single element and other responses have been received from other networked element on the same subnetwork within a predetermined amount of time.
4. A method of producing failure alerts in a computer network as set forth in Claim 2, wherein the step of performing fault tree analysis further comprises
15 the step of determining that a router interface, network interface card or port is failed only if no responses have been received from any of the networked elements on the subnetwork associated with that router interface, network interface card or port, and only if other responses have been received from
20 other networked elements on other subnetworks associated with other router interfaces, network interface cards, and ports on the same router within a predetermined amount of time.

5. A method of producing failure alerts in a computer network as set forth in Claim 2, wherein the step of performing fault tree analysis further comprises the step of determining that a router is failed only if no responses have been received from any networked elements on any subnetworks associated with any of the router's interfaces, network interface cards, and ports within a predetermined amount of time.
6. A method of producing failure alerts in a computer network as set forth in Claim 1, further comprising the steps of:
- receiving via a computer network one or more network element failed messages transmitted from said network management server;
- selecting one network element failed message based upon results of said fault tree analysis; and
- forwarding said selected network element failed message to said problem management server via a computer network, thereby blocking the forwarding of all other network element failed messages received from the network management server from being received by said problem management server.
7. A method of producing failure alerts in a computer network as set forth in Claim 1, further comprising the following steps after expiration of the timer and prior to performance of the fault tree analysis:
- immediately retransmitting all status query messages to all networked elements upon the expiration of the timer; and

re-initiating a timer for awaiting receipt of valid status responses from each networked element in reply to each retransmitted status query message, such that said step of performing fault tree analysis may be performed using a set of recently received responses from the networked elements.

8. A method of producing failure alerts in a computer network as set forth in Claim 7 wherein said re-initiated timer is set for an expedited expiration, its expiration value being significantly shorter than the value of its normally initiated value.
9. A computer program product for use with network management server in a computer network, said computer network containing a plurality of networked elements including at least one network router, at least one network management server, and at least one problem management server, said router being interconnected to several subnetworks, each subnetwork interconnecting several networked elements, said computer program product comprising:
- a computer usable medium having computer readable program code means embodied in said medium for monitoring transmissions via a computer network at least one status query message to each of said networked elements in said computer network;
- a computer usable medium having computer readable program code means embodied in said medium for initiating a timer for awaiting receipt of valid status responses from each networked element in reply to each

status query message;

a computer usable medium having computer readable program code means embodied in said medium for performing a fault tree analysis to determine the most likely single point of failure based upon a rule structure related to the topology of the computer network, said performance of fault tree analysis being invoked by expiration of the timer if less than all status responses are received; and

a computer usable medium having computer readable program code means embodied in said medium for transmitting via a computer network to said problem management at least one element failed message server for said determined single point of failure such that said problem management server is notified of the most likely point of failure.

10. A computer program product for use with network management server in a computer network as set forth in Claim 9 further comprising:

a computer usable medium having computer readable program code means embodied in said medium for accessing a computer-readable media disposed in said network management server to obtain computer network connectivity and topology data; and

a computer usable medium having computer readable program code means embodied in said medium for initiating said rule structure based upon said accessed computer network connectivity and topological data.

11. A computer program product for use with network management server in a computer network as set forth in Claim 9 wherein the computer readable code for performing fault tree analysis further comprises computer readable program code means embodied in said medium for determining that a single element on a subnetwork is failed only if no response has been received from that single element and other responses have been received from other networked element on the same subnetwork within a predetermined amount of time.
12. A computer program product for use with network management server in a computer network as set forth in Claim 9 wherein the computer readable code for performing fault tree analysis further comprises computer readable program code means embodied in said medium for determining that a router interface, network interface card or port is failed only if no responses have been received from any of the networked elements on the subnetwork associated with that router interface, network interface card or port, and only if other responses have been received from other networked elements on other subnetworks associated with other router interfaces, network interface cards, and ports on the same router within a predetermined amount of time.
13. A computer program product for use with network management server in a computer network as set forth in Claim 9 wherein the computer readable code for performing fault tree analysis further comprises computer readable program code means embodied in said medium for determining that a router is

failed only if no responses have been received from any networked elements on any subnetworks associated with any of the router's interfaces, network interface cards, and ports within a predetermined amount of time.

14. A computer program product for use with network management server in a computer network as set forth in Claim 9, further comprising:
- 5 a computer usable medium having computer readable program code means embodied in said medium for receiving via a computer network one or more network element failed messages transmitted from said network management server;
- 10 a computer usable medium having computer readable program code means embodied in said medium for selecting one network element failed message based upon results of said fault tree analysis; and
- a computer usable medium having computer readable program code means embodied in said medium for forwarding said selected network
- 15 element failed message to said problem management server via a computer network, thereby blocking the forwarding of all other network element failed messages received from the network management server from being received by said problem management server.

- 20 15. A computer program product for use with network management server in a computer network as set forth in Claim 9, further comprising:

a computer usable medium having computer readable program code means embodied in said medium for immediately retransmitting all status query messages to all networked elements upon the expiration of the timer; and

5 a computer usable medium having computer readable program code means embodied in said medium for re-initiating a timer for awaiting receipt of valid status responses from each networked element in reply to each retransmitted status query message, such that said fault tree analysis may be performed using a set of recently received responses from the
10 networked elements.

16. A network management server system for producing failure alerts in a computer network, said computer network having at least one network router interconnected to several subnetworks, a plurality of networked elements interconnected via said subnetworks and to said network routers, and at least
15 one problem management server for escalation of failure alerts and notification of failures to maintenance personnel, said network management server system comprising:
- a network server including a computer hardware platform with a processor and
20 computer-readable medium for storing data and program code, a network communications protocol stack, a network management software suite, and at least one means for communication to networked elements, router and problem management server via said computer

network;

a status monitor which monitors status replies from said networked elements made in response to status queries from said network management software suite;

5 a failure analyzer invoked by said network management software suite upon the failure to receive one or more status replies from said networked elements, said failure analyzer performing fault tree analysis to determine the most likely point of failure in the computer network; and

10 a problem management server notifier which transmits a network element failed message to the problem management server via a computer network, said network element failed message including an indicator corresponding to said most likely point of failure as determined by the failure analyzer.

17. A network management server system for producing failure alerts in a computer network as set forth in Claim 16, wherein said failure analyzer further comprises:

15 a set of rules for determining the most likely point of failure based upon a predetermined topological interrelationship between the networked elements, the subnetworks, and the routers and their interfaces to the subnetworks; and

20 a comparator which applies the rules to a set of information containing all the status replies received from networked elements within a

predetermined time period, said comparator producing an output
corresponding to a most likely point of failure of the network.

18. A network management server system for producing failure alerts in a
computer network as set forth in Claim 17, wherein said set of rules comprise
5 a rule that declares a networked element to be failed only if no status reply
from the networked element is found in the set of information being analyzed
by the analyzer, and only if at least one status reply from any other networked
element on the same subnetwork is found in the set of information being
analyzed by the analyzer.
- 10 19. A network management server system for producing failure alerts in a
computer network as set forth in Claim 17, wherein said set of rules comprise
a rule that declares a suspect network router interface, network interface card,
and port to be failed only if no status reply from any networked element on the
subnetwork associated with the suspect network router interface, network
15 interface card, and port is found in the set of information being analyzed by
the analyzer, and only if at least one status reply from any other networked
element on any other subnetwork associated with any other router interface,
network interface card, and port on the same network router is found in the set
of information being analyzed by the analyzer.
- 20 20. A network management server system for producing failure alerts in a
computer network as set forth in Claim 17, wherein said set of rules comprise
a rule that declares a suspect network router to be failed only if no status reply

from any networked element any subnetwork associated any network interface card or port associated with the suspect network is found in the set of information being analyzed by the analyzer.

21. A network management server system for producing failure alerts in a computer network as set forth in Claim 16 further comprising a status refresher which immediately transmits a status query message to each networked element upon the invocation of the failure analyzer in order to update the set of replies received and allow analysis on more recent status of the network to be performed.
22. A network management server system for producing failure alerts in a computer network as set forth in Claim 16 wherein said status monitor, fault analyzer and problem management server notifier are application programs interfaced to a standard network management server software suite.
23. A network management server system for producing failure alerts in a computer network as set forth in Claim 22 wherein said application programs are "C" programs compiled and targeted for execution by said computer hardware platform.
24. A network management server system for producing failure alerts in a computer network as set forth in Claim 22 wherein said standard network management server software suite is a NetView suite.

25. A network management server system for producing failure alerts in a computer network as set forth in Claim 22 wherein said standard network management server software suite is an OpenView suite.
26. A network management server system for producing failure alerts in a computer network as set forth in Claim 22 wherein said computer hardware platform is an RS/6000 computer platform running an AIX operating system, both of which are International Business Machines products.

5